Authentication m thod establishing a secured channel betwe n a subscrib r and a s rvice provid r accessed through a t lecommunication operator

Patent Number: EP1022922
Publication date: 2000-07-26

Inventor(s): WARY JEAN-PHILIPPE M (FR)
Applicant(s): SRF SA (FR)

Requested Patent: ☐ EP1022922
Application EP20000460005 20000121
Priority Number(s): FR19990000901 19990122
IPC Classification: H04Q7/38; H04L9/32
EC Classification: H04Q7/38A
Equivalents: ☐ FR2788914, ☐
Cited Documents: WO9851037

Abstract

The system includes an initial inscription process, followed by an exchange of authentication data The process provides authentication of a subscriber and establishment of a secure connection channel between a subscriber and a service provider. It includes an initial inscription process when the subscriber communicates with the service provider via the operator. The process includes an exchange of authentication data (DeviceID, R1; login, mdp) on line and off line. The encoded channel is eventually established at the start of each session, after mutual authentication, which also uses cryptographic functions. Finally an encoding key (Kses) is established without transmission of a secret element on the network(s).

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 022 922 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
26.07.2000 Bulletin 2000/30

(51) Int. Cl.[7]: **H04Q 7/38**, H04L 9/32

(21) Numéro de dépôt: **00460005.2**

(22) Date de dépôt: **21.01.2000**

(84) Etats contractants désignés:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Etats d'extension désignés:
AL LT LV MK RO SI

(30) Priorité: **22.01.1999 FR 9900901**

(71) Demandeur:
Societé Francaise du Radiotéléphone
92915 Paris la Défence (FR)

(72) Inventeur:
Wary, Jean-Philippe M.
92340 Bourg-La-Reine (FR)

(74) Mandataire: **Vidon, Patrice**
Cabinet Patrice Vidon,
Immeuble Germanium,
80, Avenue des Buttes-de-Coesmes
35700 Rennes (FR)

(54) Procédé d'authentification, avec établissement d'un canal sécurise, entre un abonné et un fournisseur de services accessible via un opérateur de télécommunications

(57) Le procédé est caractérisé en ce qu'il comprend d'une part un processus d'inscription initiale dudit abonné audit fournisseur de service via ledit opérateur, et d'autre part un processus de déroulement de chacune des sessions de communication entre l'abonné et le fournisseur de service, le processus d'inscription initiale consistant en un échange de données d'authentification (DeviceID, R1 ; login, mdp) en ligne ou hors ligne, et le canal chiffré étant ensuite éventuellement établi au début de chaque session après authentification mutuelle faisant intervenir des fonctions cryptographiques, puis un calcul d'une clé de chiffrement Kses, sans transmission d'élément secret sur le(s) réseau(x).

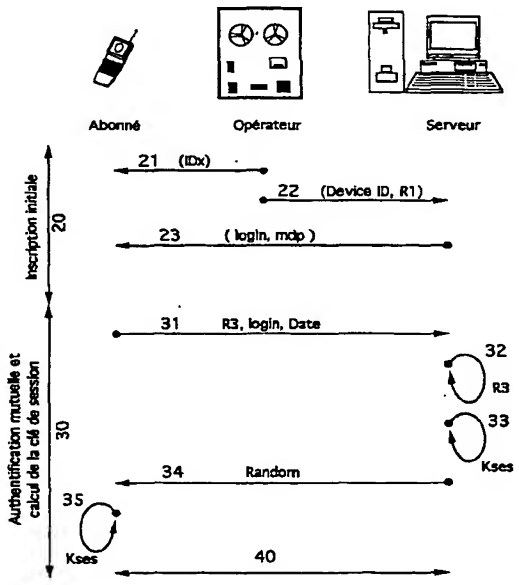

Fig. 2

EP 1 022 922 A1

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.6

Description

[0001] Le domaine de l'invention est celui de la sécurisation du transfert de données au travers d'un ou plusieurs réseaux de télécommunications.

[0002] La sécurisation s'entend ici comm étant la capacité d'assurer une authentification des parties souhaitant communiquer, puis d'établir, le cas échéant, un canal de communication sécurisé entre elles.

[0003] Il est notamment, mais non exclusivement, adapté aux applications dans lesquelles l'abonné au réseau de télécommunication se connecte par l'intermédiaire d'un téléphone mobile (ou ME pour "Mobile Equipment" en anglais), par exemple en utilisant la norme de télécommunication GSM (pour Global System for Mobile communications" en anglais), ou une norme équivalente ou concurrente telle que DCS 1800 (pour "Digital Cellular à 1800 Mhz", en anglais), PCS 1900 (pour "Personal Communication System à 1900 MHz" en anglais), DECT (pour "Digital European Cordless Telecommunications" en anglais, ou UTMS (pour "Universal Mobile Telecommunication System" en anglais).

[0004] De façon connue, ces réseaux de communication avec des mobiles sont gérés par des "opérateurs de réseau mobile", ci-après dénommés "opérateurs", qui assurent toutes les fonctions de gestion des abonnements, d'acheminement des communications, ou encore de négociation de conditions d'accès de leurs abonnés à des fournisseurs de service (ou encore "services ou serveurs de contenu") accessibles par les réseaux de communication.

[0005] Le procédé de l'invention s'applique préférentiellement au cas où l'abonné au réseau de télécommunication par terminal mobile souhaite se connecter de façon sécurisée à un correspondant, typiquement un fournisseur de service, ce dernier étant accessible sur un autre réseau de télécommunications interconnecté avec le réseau de l'abonné.

[0006] Mais en fait le procédé de sécurisation de l'invention s'applique avantageusement dans tout autre contexte dans lequel un abonné ayant souscrit à un service accessible par un réseau de télécommunication souhaite communiquer, de façon sécurisée, et sans transfert d'éléments secrets par le réseau, avec un tiers distant dans le cadre de communications de données impliquant soit un réseau unique, soit deux ou plusieurs réseaux interconnectés dont le passage de l'un à l'autre implique une rupture de protocole.

[0007] Bien que l'invention s'applique à l'origine à des communications établies entre d'une part un réseau fermé (de type GSM) auquel est rattaché l'abonné, vers un réseau ouvert (de type internet), la nature ouverte ou fermée de chacun des réseaux de transmission impliqué n'est pas une caractéristique limitative du principe général de l'invention.

[0008] Beaucoup de services de contenu sont généralement accessibles via un réseau de communication ouvert, typiquement internet, qui possède son protocole propre de communication. Lorsqu'un terminal mobile GSM souhaite accéder à un tel service, il y a donc rupture de protocole à l'interface entr le réseau GSM et le réseau d'accès au fournisseur d service de type internet. C'est d'ailleurs le rôle des opérateurs d télécommunication d'assurer et de gérer ces éléments de médiation et d'interfaçage.

[0009] Actuellement, il existe des procédés d'authentification et de confidentialité propres à chacun de ces deux réseaux. Les solutions connues consistent donc à mettre en oeuvre de façon juxtaposée les procédures disponibles sur l'un puis l'autre réseau, lors de la transmission de chaque train de données. Il en résulte généralement une rupture de confidentialité au niveau de l'interface. En particulier, la mise en oeuvre de protocoles sécurisé sur chaque segment amont et aval impose que l'opérateur soit en possession des éléments secrets, clés et/ou algorithmes cryptographiques requis par chaque procédé d'authentification et confidentialité. Cette responsabilité fait peser sur l'opérateur une contrainte de conservation de la confidentialité qui peut être indésirable pour le fournisseur de service, pour l'abonné, voire pour l'opérateur lui-même.

[0010] Une autre solution connue consiste à faire intervenir un tiers pour la gestion des secrets, habituellement nommé "tiers de confiance", mais cette solution est également lourde, et donc inappropriée à certaines situations où le coût et la complexité de gestion ne s'imposent pas.

[0011] L'invention a pour objectif de pallier ces différents inconvénients de l'état de la technique.

[0012] Plus précisément, un premier objectif de l'invention est d'assurer une procédure d'authentification qui puisse être mise en oeuvre indépendamment des réseaux successifs qu'emprunte une communication. Une telle procédure d'authentification doit pouvoir au moins permettre au fournisseur de service d'authentifier l'abonné , et préférentiellement de façon mutuelle, lors de chaque session.

[0013] L'objectif de l'invention est également de fournir un procédé de transfert de données via un canal chiffré qui permette à un abonné et un fournisseur de service de communiquer de façon sécurisée sans intervention, voire même à l'insu, de l'opérateur du réseau de rattachement de l'abonné.

[0014] Un autre objectif de l'invention est de fournir un procédé qui permette à l'opérateur de définir le schéma de sécurisation, et de garantir la qualité de l'authentification sur la liaison dont il a le contrôle, sans qu'il ait à connaître du contenu ni des éléments de fonctionnement du canal chiffré.

[0015] C'est également un objectif de l'invention que de permettre à l'abonné et au fournisseur de service de partager la connaissance d'une clé de chiffrement des messages qu'ils échangent sur le réseau, chaque clé étant avantageusement différente pour chaque session de communication, sans que la clé de chif-

frement transite à aucun moment sur le réseau.

[0016] L'invention a également pour objectif d'utiliser de façon optimisée les ressources en matière de sécurité qui sont natives d'un réseau GSM, à savoir essentiellement l'utilisation d'élément(s) secret(s) et d'algorithme(s) présents - ou le cas échéant (re)-programmables - dans les terminaux des abonnés au réseau, typiquement dans le module d'identification d'abonné, généralement dit "carte SIM" (en anglais "Subscriber Identity Module") coopérant avec le terminal radiotéléphonique de l'abonné.

[0017] Un autre objectif de l'invention est de fournir à l'abonné un mot de passe, ainsi que les moyens de calculer une clé de chiffrement/déchiffrement, qui sont attribués et gérés exclusivement par le fournisseur de services, et qui n'ont donc à être connus ni de l'opérateur, ni de tiers.

[0018] L'invention a aussi pour objectif de fournir un procédé qui assure une réelle "étanchéité" entre les différents fournisseurs de services, du point de vue de la sécurité des communications, et des transactions éventuelles initiées par l'abonné.

[0019] Ces objectifs, ainsi que d'autres qui apparaîtront par la suite sont atteints, selon l'invention, à l'aide d'un procédé de sécurisation d'une communication entre d'une part un abonné à un réseau de télécommunication et d'autre part un fournisseur de services accessible via un opérateur dudit réseau de télécommunication auquel est rattaché l'abonné, procédé caractérisé en ce qu'il comprend d'une part un processus d'inscription initiale dudit abonné audit fournisseur de service via ledit opérateur, et d'autre part un processus de déroulement de chacune des sessions de communication entre l'abonné et le fournisseur de service.

[0020] Par abonné on entend bien entendu non seulement l'utilisateur, mais aussi et surtout son équipement de réseau. De même, le fournisseur de services s'entend comme étant principalement le serveur informatique connecté au réseau. Toutefois, comme on le verra ci-après, certains transferts d'information peuvent avoir lieu hors réseau (par exemple par courrier postal, ou télécopie, etc...), et impliquer donc d'autres entités, notamment des individus, pour leur réalisation.

[0021] Selon l'invention, le processus d'inscription initiale comprend:

- d'une part la fourniture par l'opérateur de télécommunication à destination du fournisseur de service, d'un identifiant (Device ID) de l'abonné dans son réseau de rattachement, et d'un authentifiant (R1) dudit abonné formé d'une première valeur numérique calculée à partir d'un identifiant (IDx) du fournisseur de service dans le réseau de l'opérateur, dudit identifiant (Device ID) de l'abonné dans son réseau de rattachement, et d'un élément secret (Sec.Op.) caractérisant l'abonné;
- d'autre part la fourniture par le fournisseur de service à destination de l'abonné de données (login, mdp) d'identification/authentification de l'abonné auprès dudit fournisseur.

[0022] Par ailleurs, selon l'invention, le processus de déroulement de chacune desdites sessions comprend une authentification de l'abonné par le fournisseur de service au moyen des étapes suivantes:

- une étape de calcul d'une deuxième valeur numérique (R2) à partir d'un identifiant (mdp) de l'abonné auprès du fournisseur de service et d'une donnée de diversification (Date) élaborée au niveau de l'abonné
- une étape de calcul d'une troisième valeur numérique (R3) à partir de ladite première valeur numérique (R1), de ladite seconde valeur numérique (R2) et d'une troisième donnée (Login) identifiant l'abonné auprès du fournisseur de service
- une étape de transmission depuis l'abonné vers le fournisseur de service d'une première trame de données constituée de ladite troisième valeur numérique (R3) et de données d'entrée, à savoir d'une donnée (Login) identifiant l'abonné auprès du fournisseur de service, et de ladite donnée de diversification (Date) élaborée au niveau de l'abonné
- une étape d'authentification de l'abonné par le fournisseur de service par le recalcul de validation de ladite troisième valeur numérique (R3) à partir desdites données d'entrée (Login, date) de ladite première trame de données, et de données (R1, mdp) déjà à disposition du fournisseur de service et associées audit abonné.

[0023] Selon une autre caractéristique avantageuse de l'invention, le procédé comprend également une authentification du fournisseur de service par l'abonné au moyen des étapes suivantes:

- une étape de calcul d'une quatrième valeur numérique (R4) à partir dudit authentifiant (R1) de l'abonné, d'une variable aléatoire (random) élaborée au niveau du fournisseur de service et d'une donnée de diversification (Date);
- une étape de transmission depuis le fournisseur de service vers l'abonné d'une seconde trame de données constituée de ladite quatrième valeur numérique (R4) et de ladite variable aléatoire (random);
- une étape d'authentification du fournisseur de service par l'abonné par le recalcul de validation de ladite quatrième valeur numérique (R4) à partir de ladite variable aléatoire (random) de ladite seconde trame de données, et de données (R1, Date) à disposition dudit abonné.

[0024] Ainsi, dès lors qu'il respecte toutes les caractéristiques énoncées ci-dessus, le procédé permet une authentification mutuelle de l'abonné et du

fournisseur de services.

[0025] Lorsque l'authentification a été confirmée, préférentiellement d façon mutuelle, le procédé comprend en outr avantageusement:

- une phase d'élaboration d'une clé de session (Kses) commune audit d'abonné et audit fournisseur de service ; et,
- une phase de transmission de données chiffrées au moyen de ladite clé de session (Kses).

[0026] Dans ce cas, ladite phase d'élaboration d'une clé de session (Kses) comprend préférentiellement les étapes suivantes:

- une étape de calcul d'une clé de session (Kses) par le fournisseur de service à partir de données de calcul comprenant ladite seconde valeur numérique (R2) et une variable aléatoire (Random2);
- une étape de transmission à l'abonné de la seule variable aléatoire (Random2), sauf lorsque lesdites variables aléatoires Random et Random2 sont identiques, auquel cas ladite phase d'élaboration d'une clé de session (Kses) ne comprend aucune transmission de données du fournisseur de services à l'abonné, puisque cette dernière est déjà à disposition de l'abonné grâce à ladite seconde trame de données.;
- une étape de calcul par l'abonné de ladite clé de session à partir desdites données de calcul, à savoir de ladite variable aléatoire (Random2) transmise et de ladite seconde valeur numérique (R2) à disposition dudit abonné.

[0027] Dans les caractéristiques de l'invention exposées jusqu'à présent, le procédé comprend, à chaque session, les étapes successives et disjointes suivantes:

- authentification de l'abonné par le fournisseur de services;
- authentification du fournisseur de services par l'abonné;
- calcul d'une clé de session pour l'établissement d'un canal chiffré.

[0028] De cette façon on peut mettre en oeuvre sélectivement tout ou partie du procédé complet proposé.

[0029] Toutefois, dans une autre variante de réalisation, il est possible de combiner l'étape d'authentification du fournisseur de services par l'abonné avec l'étape de calcul de la clé de session pour l'établissement du canal chiffré. Selon cette variante, lesdites données de calcul de la clé de session (Kses) incluent également l'authentifiant de l'abonné (R1), ledit authentifiant (R1) étant à disposition tant dudit fournisseur de services que de l'abonné sans nécessité de sa transmission du premier au second. A ce moment, l'obtention correcte de ladite clé de session (Kses) calculé vaut authentification du fournisseur de s rvice par l'abonné du fait de l'intelligibilité des données chiffrées reçues du fournisseur de service et déchiffrées au moyen de ladite clé de session (Kses) calculée par l'abonné.

[0030] Il n'est donc plus besoin de mettre en oeuvre les calculs et transferts d'information relatifs à la quatrième variable numérique R4.

[0031] Le calcul de la clé de session, que ce soit dans le mode de réalisation à étapes disjointes, ou dans celui combinant l'authentification retour et le calcul de la clé, peut présenter en outre lui-même une variante selon laquelle lesdites données de calcul de la clé de session (Kses) incluent également la donnée de diversification (Date), étant remarqué que cette donnée de diversification (Date) est à disposition tant dudit fournisseur de services que de l'abonné et qu'il n'est donc pas nécessaire de la retransmettre du premier au second.

[0032] Ainsi, selon l'invention, et quelles qu'en soient les variantes, le schéma d'authentification mêle deux couches de sécurisation, à savoir une identification/authentification (DeviceID, R1) au niveau du réseau à une identification au niveau applicatif (login, mdp). On s'appuie donc sur la sécurité intrinsèque que peut offrir un réseau de télécommunication, au niveau de l'application, lors de l'authentification des parties et/ou de l'établissement d'une communication chiffrée.

[0033] L'authentification mutuelle repose sur la diffusion d'une valeur R1 par l'opérateur, au moment de l'insciption de l'abonné auprès du fournisseur de services, à charge pour ce dernier d'assurer la protection de cette valeur qu'il conserve dans sa base de données d'authentification. L'abonné, quant à lui, ne conserve en principe pas cette valeur R1 (pour des raisons de sécurité), mais est en mesure de la recalculer automatiquement à chaque initialisation d'une nouvelle session. A ce moment, deux échanges sont nécessaires pour que les parties s'authentifient mutuellement, et établissent un canal sécurisé.

[0034] On notera que l'établissement d'un canal chiffré ne requiert qu'une information secrète, dont la génération est sous la responsabilité de l'opérateur de rattachement, information secrète détenue par l'abonné ou confinée dans son équipement connecté au réseau.

[0035] Selon une caractéristique avantageuse de l'invention, le fournisseur de service constitue une base de données associant à chaque abonné enregistré au moins une des données suivantes:

- un identifiant (DeviceID) de l'abonné dans son réseau de rattachement;
- des données d'identification/authentification de l'abonné auprès du fournisseur de service (Login, mdp);
- la valeur numérique R1 reçue de l'opérateur au moment du processus d inscription initiale;

- le cas échéant, au moins certaines des valeurs Date, R3, R4, Random, Random2 et Kses spécifiques de la session de communication courante.

[0036] Selon une autre caractéristique de l'invention, au moins certaines desdites première, seconde et troisième (et le cas échéant quatrième) valeurs numériques R1, R2, R3, R4 et la clé de session Kses sont calculées au moyen d'un algorithme cryptographique f1, f2, f3, f4, fk. Ledit algorithme cryptographique appartient préférentiellement au groupe comprenant:

- les algorithmes à fonction de hachage à sens unique avec clé, tels que DES en mode MAC;
- les algorithmes à fonction de hachage à sens unique sans clé, tels que md5 (marque déposée), RIPEM et SHA;
- les algorithmes à mélange de bits.

[0037] Avantageusement, ladite première valeur numérique R1 est calculée au moyen d'un algorithme f1 de type A3/A8.

[0038] Selon une autre caractéristique préférentielle de l'invention, ledit élément secret (Sec. Op.) caractérisant l'abonné appartient au groupe comprenant la clé Ki contenue dans la carte SIM du mobile de l'abonné (lorsqu'on est en présence d'un réseau de type GSM) et une clé Kkm quelconque disponible dans le terminal de l'abonné.

[0039] De même, dans le cas où le réseau de rattachement de l'abonné est le réseau GSM, l'identifiant (Device ID) de l'abonné dans son réseau de rattachement appartient avantageusement au groupe comprenant l'IMSI ("International Mobile Subscriber Identity") et l'MSISDN ("Mobile Station ISDN Nr").

[0040] Préférentiellement, lesdites données (login, mdp) d'identification/authentification de l'abonné auprès dudit fournisseur sont constituées par:

- un identifiant (login) de l'abonné dans le réseau du fournisseur de service,
- un élément secret (mdp) fourni à l'abonné par le fournisseur de service.

[0041] Avantageusement, ladite donnée de diversification (Date) utilisée pour le calcul d'une deuxième valeur numérique (R2) appartient au groupe comprenant la date et/ou l'heure de la session, un nombre incrémenté à chaque nouvelle session demandée par l'abonné et un nombre aléatoire généré au niveau de l'abonné.

[0042] Avantageusement, le fournisseur de service peut s'assurer de la qualité de la donnée de diversification (Date) de l'abonné, en s'assurant qu'elle évolue effectivement dans le temps. Il peut par exemple effectuer cette vérification en conservant la valeur (Date) de la dernière tentative de connexion, pour constater si cette dernière est bien différente de la valeur (Date) courante.

[0043] Selon une version dégradée du schéma de sécurisation proposé par l'invention, ladite première valeur numérique (R1) n'est pas calculée et est ignorée à au moins certaines étapes du procédé, ladit phase d'authentification de l'abonné par le fournisseur de service étant alors supprimée. Cette simplification a pour conséquence la perte du processus d'authentification mutuelle, et rend le schéma vulnérable à des attaques du type "man in the middle" (anglais pour intrus qui s'intercale dans le communication). Mais les autres fonctions d'identification et d'authentification subsistent.

[0044] Il est également possible de simplifier l'utilisation de la deuxième valeur numérique R2, en la réduisant simplement à la valeur de l'élément secret (mdp) fourni à l'abonné par le fournisseur de services. Dans ce cas, cette valeur n'est plus "dynamique" (c'est à dire variable en fonction des occurrences), mais figée. La fonction cryptographique f2 n'est alors bien entendu pas utilisée.

[0045] D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante d'un mode de réalisation illustratif et non limitatif de l'invention, et des dessins annexés dans lesquels:

- la figure 1 schématise un exemple de configuration de réseaux de communication au sein de laquelle peut être mise en oeuvre l'invention;
- la figure 2 illustre schématiquement les phases successives de la variante du procédé de sécurisation selon l'invention, dans laquelle l'authentification retour est combinée au calcul de la clé de session;
- la figure 3 représente les étapes principales de calcul des valeurs numériques utilisées dans le cadre du procédé de transfert de données sécurisé selon l'invention.

[0046] La configuration de la figure 1 est constituée d'un premier réseau de communication 11, géré par un opérateur 12, et comportant un abonné 13. Pour illustrer plus précisément cette configuration, on peut considérer que le réseau 11 est un réseau fermé à abonnement, du type d'un réseau GSM. L'abonné 13 est muni d'un téléphone mobile, typiquement un terminal portable muni d'une carte "SIM", communiquant avec le réseau 11 via une station de base (BTS). Le même opérateur 12 assure aussi par exemple la gestion d'un intranet, sur lequel est connecté un second abonné 14. Cet abonné 14 communique au moyen d'un ordinateur 18, connecté au réseau via un modem 19.

[0047] Sur demande d'un abonné, l'opérateur 12 est en mesure de réaliser une interconnexion 15 vers un second réseau 16, qui comprend lui-même un certain nombre d'utilisateurs, dont un fournisseur de services en ligne 17.

[0048] Le réseau 16, quant à lui, est par exemple un réseau ouvert du type internet, utilisant le protocole de communication IP. Le fournisseur de services en ligne

17 est un service de contenu accessible moyennant un processus préalable d'inscription auprès du service. Il s'agit par exemple d'un site bancaire, mis à la disposition de ses clients par une banque, et qui leur permet de consulter leurs comptes et/ou d'effectuer des transactions à distance. Ces opérations ont une nature confidentielle qui requiert d'une part que les interlocuteurs (le client abonné d'une part et la banque d'autre part) authentifient mutuellement leur identité afin d'éviter toute fraude, et d'autre part que les échanges d'information s'effectuent de façon chiffrée pour faire échec aux ruptures de confidentialité.

[0049] Chaque connexion d'un abonné client au fournisseur de service en ligne initie une session de communication dont l'établissement et le déroulement suivent le procédé de transfert de données par canal sécurisé selon l'invention.

[0050] Selon l'invention, l'établissement d'un canal sécurisé nécessite que l'abonné soit préalablement inscrit auprès du fournisseur de services, et que l'opérateur ait transmis au fournisseur de services des données servant à l'identification et l'authentification abonné/fournisseur, utilisées lors de l'établissement ultérieur de sessions de communication. En revanche, l'établissement et l'utilisation du canal sécurisé se passent sans intervention de l'opérateur du réseau de l'abonné, si ce n'est bien entendu au niveau du transport de la communication brute, celle-ci restant indéchiffrée et indéchiffrable par l'opérateur puisque les élements secrets ne sont connus que de l'abonné et du fournisseur de services. L'opérateur se contente de définir le schéma de sécurisation, c'est à dire de permettre la mise en oeuvre de l'invention. L'opérateur garantit la qualité de ce schéma pour les services d'authentification et de confidentialité. En revanche, bien entendu, le fournisseur de service reste responsable de la continuité de la chaine de sécurisation à son propre niveau.

[0051] Dans le schéma de la figure 2 apparaissent successivement les deux processus consécutifs de mise en oeuvre du procédé de l'invention, à savoir:

- un premier processus 20 de souscription initiale dudit abonné audit fournisseur de service via ledit opérateur,
- un second processus 30 de déroulement de chacune des sessions de communication entre l'abonné et le fournisseur de service.

[0052] Lors du premier processus 20 d'inscription (ou souscription), on retrouve essentiellement les échanges de données suivants.

[0053] Dans un premier temps, l'opérateur de télécommunication va adresser (21) à l'abonné un identifiant du fournisseur de service (IDx), auprès duquel l'abonné souhaite s'inscrire. L'identifiant IDx est unique pour chaque fournisseur de services accessible à partir du réseau de l'opérateur selon le schéma de sécurisation de l'invention. Lorsque le fournisseur de services est accessible sur un réseau de type internet, l'identifiant IDx peut par exemple êtr une URL (en anglais "Uniform Resource Locator").

[0054] L'opérateur va par ailleurs acheminer (22) vers le fournisseur de service considéré un jeu de deux données, à savoir:

- un identifiant (Device ID) de l'abonné dans son réseau de rattachement, et
- un authentifiant (R1) dudit abonné, qui est avantageusement calculé dans des conditions détaillées en relation avec la description ci-après de la figure 3.

[0055] L'authentifiant R1 est calculé à partir d'un ensemble de valeurs, uniques, dans le réseau de l'opérateur, et est donc spécifique de la liaison entre l'abonné spécifique et le fournisseur de services spécifique considérés, et à ce titre devra être protégé par le fournisseur de services. Cette valeur R1 sera donc différente, pour un abonné donné, suivant le fournisseur de service. L'authentifiant R1 sera stocké en permanence dans la base d'authentification du fournisseur de services.

[0056] En retour, le fournisseur de service va fournir (23) à l'abonné également deux données d'identification de l'abonné auprès dudit fournisseur, à savoir:

- un identifiant (login) de l'abonné dans le réseau du fournisseur de service, et
- un élément secret (mdp), sous forme par exemple d'un mot de passe.

[0057] Tout ou partie des données échangées à ce stade peuvent transiter avantageusement hors ligne de communication (en anglais "off-line") suivant des procédures propres à chacun des intervenants (par exemple par télécopie, ou courrier ou tout autre moyen). Mais il peut aussi être plus simple dans certains cas de les transmettre en ligne.

[0058] Dans le second processus 30 de déroulement de chacune des sessions de communication entre l'abonné et le fournisseur de service, on peut distinguer plusieurs phases successives.

[0059] Tout d'abord, l'abonné va s'authentifier auprès du fournisseur de service en lui adressant (31) une trame de données constituée d'une valeur numérique (R3) et d'un jeu de deux données d'entrée, à savoir la donnée (Login) qui identifie l'abonné auprès du fournisseur de service, et une donnée de diversification (Date) élaborée au niveau de l'abonné.

[0060] Cet envoi de trame fait suite immédiatement à la saisie par l'abonné, par exemple sur la clavier de son terminal de télécommunication, du couple de valeur (login,mdp) l'identifiant et l'authentifiant auprès du fournisseur de services. La valeur login est intégrée directement dans la trame précitée envoyée au fournisseur de

services, alors que la valeur mdp n'est pas transmis , mais est utilisée dans le calcul d la valeur numérique R3.

[0061] Les modalités de calcul de la valeur numériqu R3 sont détaillées en relation avec la description de la figure 3 ci-après.

[0062] La donnée de diversification peut être toute donnée assurant la variabilité et interdisant le rejeu des données fournies à l'itération précédente par l'abonné. L'objectif est bien entendu de faire échec à des tentatives d'intrusion dites de "rejeu" (en anglais "replay attack"), dans lesquelles un intervenant tiers essaierait de se faire passer pour l'abonné. La donnée de diversification est avantageusement constituée de la date et/ou de l'heure de la session, mais peut tout aussi bien être un nombre incrémenté par l'abonné à chaque nouvelle session, ou encore un nombre aléatoire ou pseudo-aléatoire généré au niveau de l'abonné.

[0063] A réception de la trame envoyée à l'étape 31, le fournisseur de services va authentifier (32) l'abonné en recalculant, pour validation, ladite troisième valeur numérique (R3) à partir desdites données d'entrée (login, date) de ladite trame de données, et de données d'authentification (R1, mdp) déjà connues du fournisseur de services et associées audit abonné. L'obtention par le fournisseur de services, lors de ce recalcul de validation, d'une valeur identique à celle de R3 reçue de l'abonné, valide et authentifie l'abonné.

[0064] L'étape suivante 33 consiste, pour le fournisseur de services, à élaborer une clé de session (Kses) à partir d'un certain nombre de données (voir ci-après), y inclus une variable aléatoire (Random). A ce moment, le fournisseur de services va se limiter à transmettre (34) à l'abonné la seule variable aléatoire (Random), qui va servir à l'abonné pour recalculer (35) de son côté la même clé de session (Kses). Ce calcul, s'il est exact, permet alors à l'abonné d'authentifier le fournisseur de service, du fait de l'intelligibilité des données chiffrées reçues du fournisseur de service et déchiffrées au moyen de ladite clé de session (Kses) calculée par l'abonné.

[0065] L'abonné et le fournisseur de services peuvent alors communiquer (40) de façon sécurisée dans le canal chiffré établi.

[0066] Ce mode de réalisation illustré en figure ne constitue que l'une des variantes de l'invention, à savoir celle dans laquelle authentification en retour (c'est-à-dire authentification du fournisseur de services par l'abonné) et calcul de la clé de session sont combinées. L'homme de l'art concevra aisément les autres variantes à partir de cet exemple illustratif.

[0067] La figure 3 représente les principales étapes de calcul des valeurs numériques effectuées au cours des processus d'inscription initiale d'un abonné, puis d'authentification et de chiffrement des communications établies entre l'abonné et le fournisseur de service.

[0068] La première valeur numérique R1 est calculée à l'aide d'un algorithme de chiffrement f1, par exemple de type A3/A8, MD5 ou DES, en utilisant préférentiellement les valeurs d'entrée suivantes:

- la valeur "IDx" identifiant l fournisseur de service dans le réseau de rattachement de l'abonné. Cet identifiant est par exemple défini par l'opérateur du réseau, qui référence ainsi par différentes valeurs différents fournisseurs de services accessibles par l'abonné. Comme déjà mentionné, chaque fournisseur de service "x" est identifié par une valeur "IDx" différente.
- la valeur "Device ID" identifiant l'abonné dans son réseau de rattachement, constituée par exemple par le nom de l'abonné, ou tout autre identifiant de l'abonné attribué par l'opérateur. L'identifiant (Device ID) de l'abonné peut aussi par exemple être constitué par son IMSI ("International Mobile Subscriber Identity") ou encore son numéro MSISDN ("Mobile Station ISDN Number").
- un élément secret (Sec Opé) authentifiant l'abonné dans le réseau de l'opérateur. Cet élément secret peut par exemple être un mot de passe, un code de type PIN (en anglais "Personal Identity Code"), ou une clé confinée au niveau de l'équipement réseau. Dans le cas d'un réseau GSM, l'élément secret en question est avantageusement la clé Ki confinée dans la carte SIM. Mais tout autre élément secret peut être accepté comme valeur d'entrée servant à calculer R1, comme par exemple une clé spécifique Kkm, dédiée à l'authentification des abonnés GSM auprès de l'ensemble des serveurs de contenu. Dans le cas où le terminal de l'abonné est un ordinateur (de type PC (ordinateur personnel) ou autre), on peut également utiliser une clé "hardware" (terme anglais pour "matériel").

[0069] La valeur R1 est calculée selon la formule R1 = f1(DeviceID, IDx, Sec. Ope). L'algorithme cryptographique A3A8 est particulièrement adapté dans la mesure où, selon la mise en oeuvre des normes GSM, il est déjà présent dans la carte SIM. Dans ce cas R1 = f1(DeviceID, IDx, Ki), et est avantageusement exprimé sur douze octets avec f1 = A3A8. Il présente donc l'avantage de minimiser les développements, d'être secret pour les tiers, et de correspondre à un niveau de sécurité cohérent avec le réseau de rattachement. Tout autre algorithme déjà présent sur la carte SIM, comme l'est généralement l'algorithme DES, est également avantageux. D'autres algorithmes cryptographiques sont également envisageables.

[0070] L'équipement de l'abonné, qui dans le cas d'un réseau GSM est le terminal GSM muni de sa carte SIM et d'un logiciel de navigation approprié, est capable de calculer automatiquement la valeur R1 lorsque l'abonné choisit d'accéder à un fournisseur de services spécifique, après bien entendu que l'abonné s'est authentifié auprès de son opérateur de réseau.

[0071] La seconde valeur numérique R2 est calcu-

lée selon la formule R2 = f2(date, mdp), dans laquelle:

- l'agorithm f2 st tout algorithme cryptographique adéquat. De préférence, il s'agit d'un algorithme effectuant un calcul de sceau par l'intermédiaire d'une fonction de hachage à sens unique. Typiquement, il peut s'agir d'un algorithme à clé, tels que DES en mode MAC, ou encore d'un algorithme sans clé, tel que md5 (marque déposée pour un algorithme de compression commercialisé par la société RSA Inc.) RIPEM ou SHA. Ces algorithmes ne sont pas limitatifs de l'invention.
  Ainsi, il est aussi possible d'utiliser un algorithme à mélange de bits, mais cette possibilité représente néanmoins une solution faible au sens cryptographique.
- la valeur (date) est la donnée de diversification discutée plus haut;
- la valeur mdp est l'élément secret adressé à l'étape 23 à l'abonné par le fournisseur de services, mais que le fournisseur de services a conservé également dans sa base d'authentification.

[0072] Cette valeur R2 n'est pas transmise en tant que telle au fournisseur de services. Il s'agit d'une variable intermédiaire, qui est utilisée pour le calcul de la valeur numérique R3. Cette valeur R2 peut d'ailleurs sans inconvénient être stockée en mémoire au niveau de l'équipement terminal de l'abonné, si celui-ci en est pourvu (par exemple dans un cache mémoire). Le fait de conserver la valeur R2 n'altère en rien, en effet, la sécurité du processus.

[0073] La troisième valeur numérique R3 est calculée selon la formule R3 = f3(R1, R2, login), dans laquelle:

- la valeur numérique R1 est l'authentifiant dudit abonné calculé comme détaillé ci-dessus, et adressée au fournisseur de services lors du processus de souscription;
- les modalités de calcul de la valeur numérique R2 ont également été précisées cidessus;
- la valeur login est l'identifiant de l'abonné dans le réseau du fournisseur de service, et retransmise par l'abonné au fournisseur de services au sein de la trame de données acheminée à l'étape 31 de la figure 2;
- l'algorithme f3 est avantageusement identique à celui choisi pour f2. En tout état de cause, il peut être choisi parmi les mêmes possibilités évoquées pour f2.

[0074] La clé de session Kses peut s'exprimer sous la forme Kses = fk(R1, R2, Random), dans laquelle:

- l'algorithme fk est avantageusement identique à celui choisi pour f2 et f3. En tout état de cause, il peut être choisi parmi les mêmes possibilités évoquées pour f2;
- les valeurs numériques R1 et R2 sont cell s déjà mentionnées;
- la val ur aléatoire ou pseudo-aléatoire Random choisie par le fournisseur de

services. Dans une version dégradée du procédé de transfert de données sécurisé, également couvert par l'invention, la valeur R1 n'est ni calculée, ni utilisée à aucun stade du procédé. Il en résulte que l'authentification du fournisseur par l'abonné n'est plus assurée, ce qui rend la sécurité de la communication plus vulnérable à des intrusions du type "man in the middle" (en anglais: "intervenant s'interposant dans la communication").

Revendications

1. Procédé de sécurisation d'une communication entre d'une part un abonné à un réseau de télécommunication et d'autre part un fournisseur de services accessible via un opérateur dudit réseau de télécommunication auquel est rattaché l'abonné,
   caractérisé en ce qu'il comprend d'une part un processus d'inscription initiale dudit abonné audit fournisseur de service via ledit opérateur, et d'autre part un processus de déroulement de chacune des sessions de communication entre l'abonné et le fournisseur de service,
   en ce que le processus d'inscription initiale comprend:

   - d'une part la fourniture par l'opérateur de télécommunication à destination du fournisseur de service,
     . d'un identifiant (Device ID) de l'abonné dans son réseau de rattachement, et
     . d'un authentifiant (R1) dudit abonné formé d'une première valeur numérique calculée à partir d'un identifiant (IDx) du fournisseur de service dans le réseau de l'opérateur, dudit identifiant (Device ID) de l'abonné dans son réseau de rattachement, et d'un élément secret (Sec.Op.) caractérisant l'abonné;
   - d'autre part la fourniture par le fournisseur de service à destination de l'abonné de données (login, mdp) d'identification/authentification de l'abonné auprès dudit fournisseur;

   et en ce que le processus de déroulement de chacune desdites sessions comprend une authentification de l'abonné par le fournisseur de service au moyen des étapes suivantes:

   - une étape de calcul d'une deuxième valeur

numérique (R2) à partir d'un identifiant (mdp) de l'abonné auprès du fournisseur de service et d'une donnée de diversification (Date) élaborée au niveau de l'abonné

- une étape de calcul d'une troisièm valeur numérique (R3) à partir de ladite première valeur numérique (R1), de ladite seconde valeur numérique (R2) et d'une troisième donnée (Login) identifiant l'abonné auprès du fournisseur de service
- une étape de transmission depuis l'abonné vers le fournisseur de service d'une première trame de données constituée de ladite troisième valeur numérique (R3) et de données d'entrée, à savoir d'une donnée (Login) identifiant l'abonné auprès du fournisseur de service, et de ladite donnée de diversification (Date) élaborée au niveau de l'abonné
- une étape d'authentification de l'abonné par le fournisseur de service par le recalcul de validation de ladite troisième valeur numérique (R3) à partir desdites données d'entrée (Login, date) de ladite première trame de données, et de données (R1, mdp) déjà à disposition du fournisseur de service et associées audit abonné.

2. Procédé selon la revendication 1 caractérisé en ce qu'il comprend également une authentification du fournisseur de service par l'abonné au moyen des étapes suivantes :

   - une étape de calcul d'une quatrième valeur numérique (R4) à partir dudit authentifiant (R1) de l'abonné, d'une variable aléatoire (random) élaborée au niveau du fournisseur de service et d'une donnée de diversification (Date);
   - une étape de transmission depuis le fournisseur de service vers l'abonné d'une seconde trame de données constituée de ladite quatrième valeur numérique (R4) et de ladite variable aléatoire (random);
   - une étape d'authentification du fournisseur de service par l'abonné par le recalcul de validation de ladite quatrième valeur numérique (R4) à partir de ladite variable aléatoire (random) de ladite seconde trame de données, et de données (R1, Date) à disposition dudit abonné.

3. Procédé selon l'une quelconque des revendications 1 et 2 caractérisé en ce qu'il comprend en outre:

   - une phase d'élaboration d'une clé de session (Kses) commune audit d'abonné et audit fournisseur de service; et,
   - une phase de transmission de données chiffrées au moyen de ladite clé de session (Kses);

   et en ce que ladite phase d'élaboration d'une clé de session (Kses) comprend les étapes suivantes:

   - une étape de calcul d'une clé de session (Kses) par le fournisseur de service à partir de données de calcul comprenant ladite seconde valeur numérique (R2) et une variable aléatoire (Random2);
   - une étape de transmission à l'abonné de la seule variable aléatoire (Random2);
   - une étape de calcul par l'abonné de ladite clé de session à partir desdites données de calcul, à savoir de ladite variable aléatoire (Random2) transmise et de ladite seconde valeur numérique (R2) à disposition dudit abonné.

4. Procédé selon les revendications 2 et 3, caractérisé en ce que lesdites variables aléatoires Random et Random2 sont identiques, et en ce que ladite phase d'élaboration d'une clé de session (Kses) ne comprend aucune transmission de données du fournisseur de services à l'abonné, ladite variable aléatoire étant déjà à disposition de l'abonné grâce à ladite seconde trame de données.

5. Procédé selon la revendication 3, sans mise en oeuvre de la revendication 2, caractérisé en ce que lesdites données de calcul de la clé de session (Kses) incluent également l'authentifiant de l'abonné (R1), ledit authentifiant (R1) étant à disposition tant dudit fournisseur de services que de l'abonné sans nécessité de sa transmission du premier au second,
   et en ce que l'obtention correcte de ladite clé de session (Kses) calculée vaut authentification du fournisseur de service par l'abonné du fait de l'intelligibilité des données chiffrées reçues du fournisseur de service et déchiffrées au moyen de ladite clé de session (Kses) calculée par l'abonné.

6. Procédé selon l'une quelconque des revendications 1 à 5 caractérisé en ce que lesdites données de calcul de la clé de session (Kses) incluent également la donnée de diversification (Date), ladite donnée de diversification (Date) étant à disposition tant dudit fournisseur de services que de l'abonné sans nécessité de sa transmission du premier au second.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que le fournisseur de service constitue une base de données associant à chaque abonné enregistré:

   - un identifiant (DeviceID) de l'abonné dans son réseau de rattachement;
   - des données d'identification/authentification de l'abonné auprès du fournisseur de service

(Login, mdp);

- la valeur numérique R1 reçue de l'opérat ur au moment du processus d'inscription initiale;
- le cas échéant, au moins certaines des valeurs Date, R3, Random, Random2 et Kses spécifiques de la session de communication courante.

8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'au moins certaines desdites première, seconde, troisième et quatrième valeurs numériques R1, R2, R3, R4, ainsi que la clé de session Kses sont calculées au moyen d'un algorithme cryptographique f1, f2, f3, fk.

9. Procédé selon la revendication 8, caractérisé en ce que ladite première valeur numérique R1 est calculée au moyen d'un algorithme f1 de type A3/A8.

10. Procédé selon la revendication 8, caractérisé en ce que ledit algorithme cryptographique appartient au groupe comprenant:

- les algorithmes à fonction de hachage à sens unique avec clé, tels que DES en mode MAC;
- les algorithmes à fonction de hachage à sens unique sans clé, tels que md5 (marque déposée), RIPEM et SHA;
- les algorithmes à mélange de bits.

11. Procédé selon l'une quelconque des revendications 1 à 10, caractérisé en ce que ledit élément secret (Sec. Op.) caractérisant l'abonné appartient au groupe comprenant la clé Ki contenue dans la carte SIM du mobile de l'abonné et une clé Kkm quelconque disponible dans le terminal de l'abonné

12. Procédé selon l'une quelconque des revendications 1 à 11, caractérisé en ce que dans le cas où le réseau de ratachement de l'abonné est le réseau GSM, l'identifiant (Device ID) de l'abonné dans son réseau de rattachement appartient au groupe comprenant l'IMSI ("International Mobile Subscriber Identity") et l'MSISDN ("Mobile Station ISDN Nr").

13. Procédé selon l'une quelconque des revendications 1 à 12, caractérisé en ce que lesdites données (login, mdp) d'identification/authentification de l'abonné auprès dudit fournisseur sont constituées par:

- un identifiant (login) de l'abonné dans le réseau du fournisseur de service,
- un élément secret (mdp) fourni à l'abonné par le fournisseur de service.

14. Procédé selon l'une quelconque des revendications 1 à 13, caractérisé en ce que ladite donnée de diversification (Date) utilisée pour le calcul d'un deuxième valeur numérique (R2) appartient au groupe comprenant la date et/ou l'heure de la session, un nombre incrémenté à chaque nouvelle session demandée par l'abonné et un nombre aléatoire généré au niveau de l'abonné.

15. Procédé selon l'une quelconque des revendications 1 à 14, caractérisé en ce que ladite première valeur numérique (R1) formant authentifiant de l'abonné est élaborée lors de chaque session, et n'est pas conservée par l'abonné.

16. Procédé de transfert de données selon l'une quelconque des revendications précédentes, dans lequel ladite première valeur numérique (R1) n'est pas calculée et est ignorée à au moins certaines étapes du procédé, ladite phase d'authentification de l'abonné par le fournisseur de service étant alors supprimée.

17. Procédé selon l'une quelconque des revendications 1 à 16, caractérisé en ce que au moins certaines des données (Device ID, R1 ; login, mdp) échangées lors de la phase de souscription initiale de l'abonné auprès du fournisseur de service sont transmises selon un moyen comprenant les transmissions en ligne et les transmissions hors ligne.

18. Procédé selon l'une quelconque des revendications 1 à 17 caractérisé en ce que ladite seconde valeur numérique (R2) est simplement égale audit élément secret (mdp) fourni à l'abonné par le fournisseur de service.

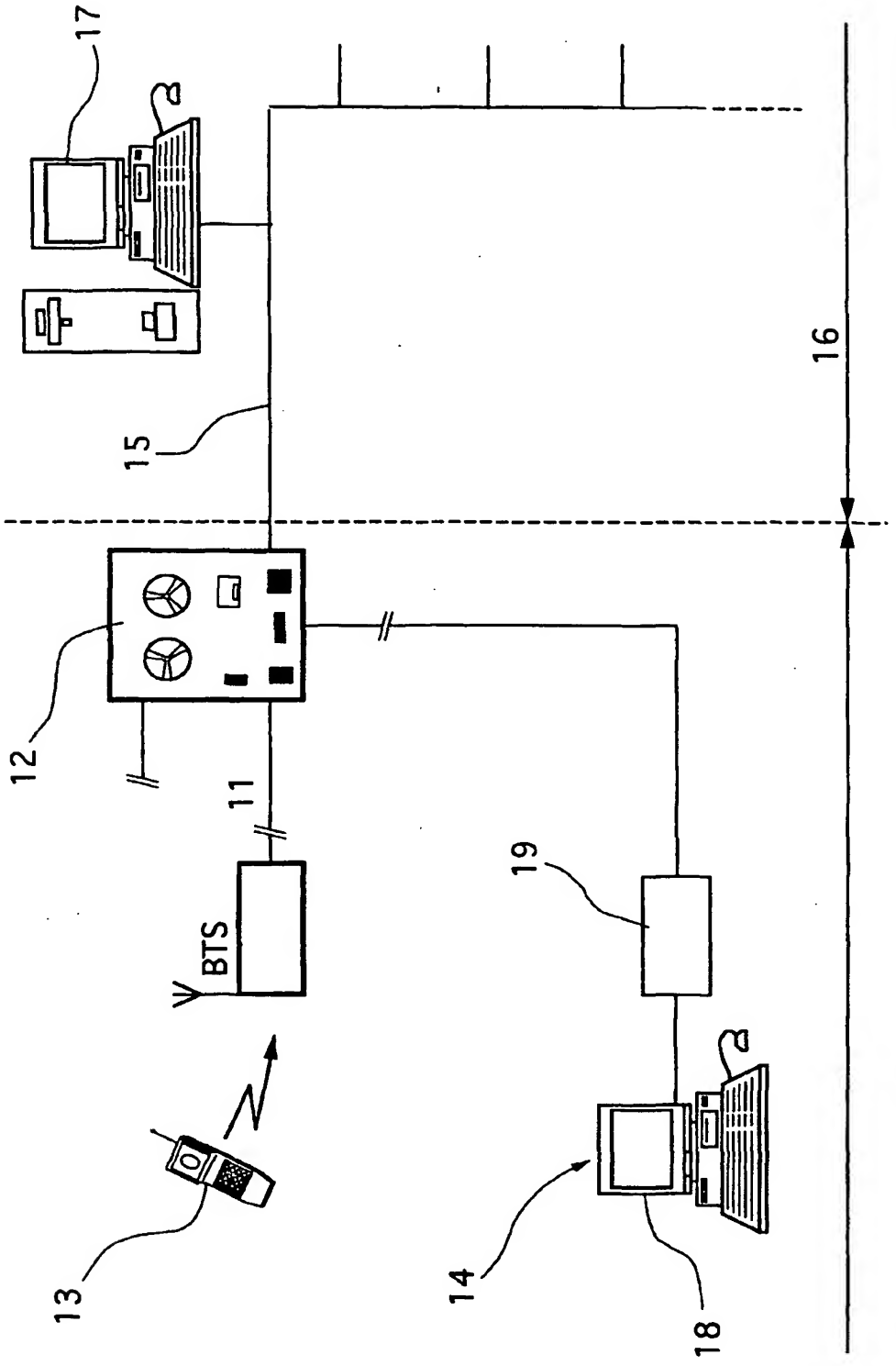

Fig. 1

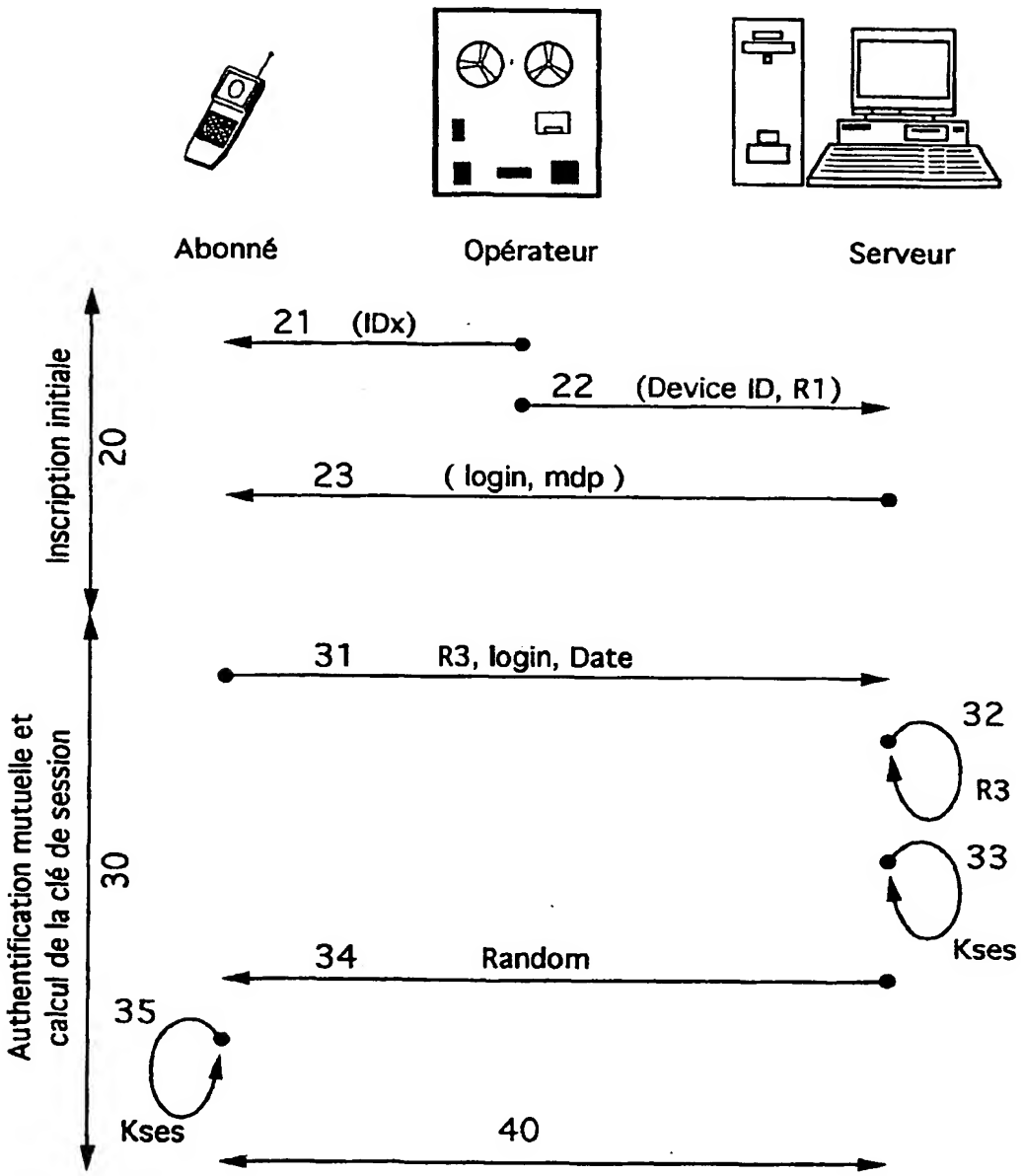
Abonné
Opérateur
Serveur
Inscription initiale
20
21 (IDx)
22 (Device ID, R1)
23 (login, mdp)
Authentification mutuelle et calcul de la clé de session
30
31 R3, login, Date
32
R3
33
Kses
34 Random
35
Kses
40

Fig. 2

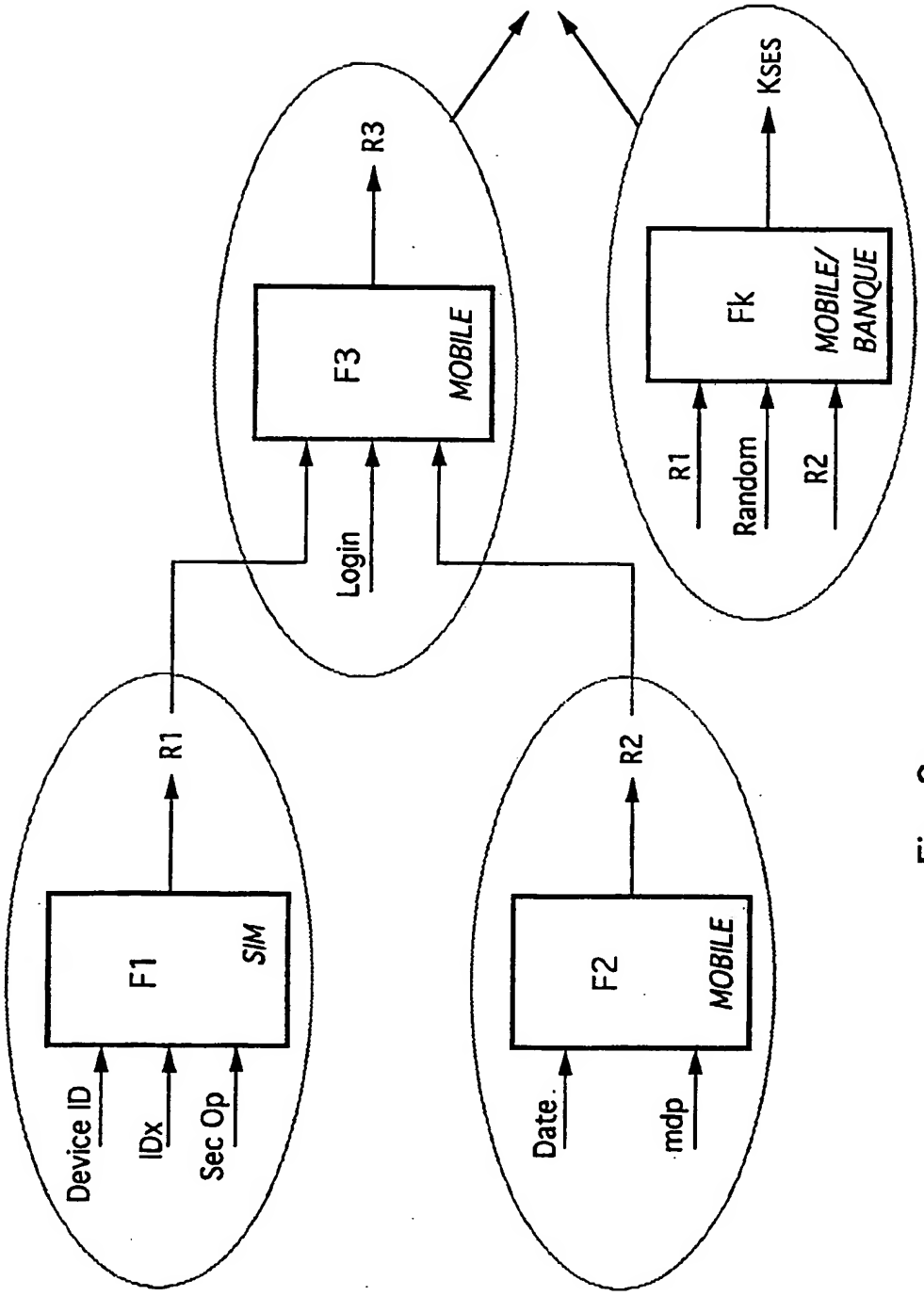
Device ID
IDx
Sec Op
F1
SIM
R1
Date
mdp
F2
MOBILE
R2
Login
F3
MOBILE
R3
R1
Random
R2
Fk
MOBILE/
BANQUE
KSES

Fig. 3

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 00 46 0005

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
X	WALKER M: "SECURITY IN MOBILE AND CORDLESS TELECOMMUNICATIONS" PROCEEDINGS OF THE ANNUAL EUROPEAN CONFERENCE ON COMPUTER SYSTEMS A SOFTWARE ENGINEERING (COMPEURO), THE HAGUE, MAY 4 - 8, 1992, no. CONF. 6, 4 mai 1992 (1992-05-04), pages 493-496, XP000344244 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS ISBN: 0-8186-2760-3	16	H04Q7/38 H04L9/32
A	* page 494, colonne de gauche, ligne 8 - colonne de droite, ligne 29 *	1	
X	MOLVA R ET AL: "AUTHENTICATION OF MOBILE USERS" IEEE NETWORK: THE MAGAZINE OF COMPUTER COMMUNICATIONS, vol. 8, no. 2, 1 mars 1994 (1994-03-01), pages 26-34, XP000515077 ISSN: 0890-8044	16	
A	* page 27, colonne de droite, ligne 36 - page 28, colonne de droite, ligne 7 *	1	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7) H04Q H04L
A	WO 98 51037 A (CERTICOM CORP ;VANSTONE SCOTT A (CA); JOHNSON DONALD B (US)) 12 novembre 1998 (1998-11-12) * page 2, ligne 30 - page 4, ligne 6 *	1	

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
BERLIN	14 avril 2000	Bernedo Azpiri, P

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 00 46 0005

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

14-04-2000

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9851037 A	12-11-1998	AU 7201798 A	27-11-1998

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82